Cloud Computing

Ferguson-Boucher, Kirsten

Published in:
IEEE Security & Privacy

DOI:
10.1109/MSP.2011.159

Publication date:
2011

Citation for published version (APA):
Ferguson-Boucher, K. (2011). Cloud Computing: A Records and Information Management Perspective. *IEEE Security & Privacy*, *9*(6), 63-66. https://doi.org/10.1109/MSP.2011.159

Editors: Deborah A. Frincke, dafrinc@nsa.gov
Richard Ford, rford@se.fit.edu

Cloud Computing: A Records and Information Management Perspective

Kirsten Ferguson-Boucher
Aberystwyth University, Wales

For many records and information management (RIM) professionals, cloud computing resembles a traditional hosting service: information storage or applications are outsourced to a third-party provider and accessed by the organization through a network connection. However, the information, applications, and processing power in a cloud infrastructure are distributed across many servers and stored along with other customers' information, separated only by logical isolation mechanisms. This presents both new RIM challenges and benefits.

RIM professionals are specifically concerned with information as a core business asset. Records are a subset of organizational information that is often required to provide evidence of organizational activities and transactions. They require protection in the same way as every other asset. Decision-making processes take into consideration the wider context of organizational strategy and form part of a complex structure of assessments regarding information value, alignment, and assurance. All of these operate within an overarching performance and risk framework.

Cloud Computing: A Brief Introduction

Cloud computing is the ability to access a pool of computing resources owned and maintained by a third party via the Internet. It isn't a new technology but a new way of delivering computing resources based on long existing technologies such as server virtualization. The "cloud" is composed of hardware, storage, networks, interfaces, and services that provide the means through which users access the infrastructure, computing power, applications, and services on demand and independent of location. Cloud computing usually involves the transfer, storage, and processing of information on the provider's infrastructure, which is outside the customer's control.

The National Institute of Standards and Security (NIST) defines it as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (http://csrc.nist.gov/publications/PubsSPs.html#800-145/SP800-145.pdf). As Figure 1 shows, the NIST-defined model highlights five essential characteristics that reflect a service's flexibility and the control that users have over it. NIST also distinguishes among three delivery models (software as a service [SaaS], platform as a service [PaaS], and infrastructure as a service [IaaS]) and four deployment models (public, private, hybrid, and community clouds).

Delivery Models

As a general rule, the customer doesn't control the underlying cloud infrastructure in any delivery model. SaaS is software offered by a third-party provider, usually on demand via the Internet and configurable remotely. PaaS also allows customers to develop new applications using APIs deployed and configurable remotely. In this case, the customer does have control over the deployed applications and operating systems. In the IaaS provision, virtual machines and other abstracted hardware and operating systems are made available. The customer, therefore, has control over operating systems, storage, and deployed applications.

Deployment Models

There are, essentially, three deployment models: private, community, and public, with a fourth "combined" option. *Private clouds* are operated solely for an organization; *community clouds* are shared by several organizations and are designed to support a specific community. In *public clouds,* the

 1540-7993/11/$26.00 © 2011 IEEE COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES

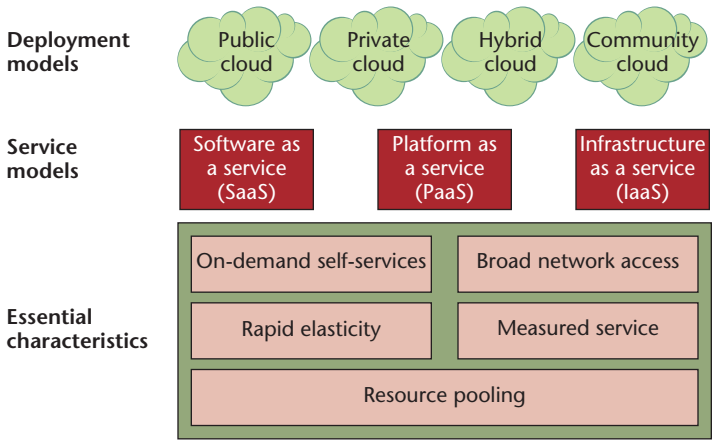

Figure 1. NIST-defined cloud computing model. The cloud enables ubiquitous, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

infrastructure is made publicly available but is owned by an organization selling cloud services. Resources are offsite and shared among all customers in a multitenancy model. *Hybrid clouds* are a composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology to enable data and application portability.

Is the Cloud Right for You?

Making the decision to move to the cloud is a complex one and depends very much on your organizational context. Let's examine some generic benefits and challenges. An obvious benefit is a reduction in capital expenditure—heavy investment in new hardware and software is no longer required for often underutilized functions, such as storage and processing. Organizations can tap into readily available computing resources on demand, with large datacenters often using virtualization technologies (the abstraction of computing resources from the underlying hardware) to enable scalable and flexible service provision. Applications, storage, servers, and networks are allocated flexibly in a multitenancy environment to achieve maximum computing and storage capacities.

From a provider perspective, utilization of shared resources results in higher efficiency and the ability to offer cloud computing services at low costs; customers likewise benefit from cheaper access. But make no mistake—the cloud still involves costs to an organization as it tries to integrate new services with existing legacy processes. Table 1 summarizes these and some of the other general pros and cons of cloud provision.

There are, however, very specific considerations that relate to the ability of the organization to manage its information and ensure that records are available for current and future organizational use. In particular, the cloud offers specific benefits for RIM: improved business processes, facilitation of location-independent collaboration, and access to resources and information at any time. However, some aspects of cloud computing can have a negative impact on RIM as well:

- compliance and e-discovery;
- integrity and confidentiality;
- service availability and reliability;
- service portability and interoperability;
- information retrieval and destruction; and
- loss of governance, integration, and management.

The sidebar "Ten Questions to Ask When Outsourcing to the Cloud" offers some guidance about what service might be best for a particular organization's context.

Managing Information Assets in the Cloud

Organizations are still responsible for their information even if it's stored elsewhere (in this case, in the cloud). ISO 15489 (the international standard for records management) defines records as being authentic, reliable, and usable and possessing integrity. How does the move to the cloud affect these characteristics? Information governance and assurance require policies and procedures for maintaining the above and will need amending to incorporate the changing environment. There must be a clear understanding of who's responsible for what and how policies and procedures will be implemented. Issues such as metadata application, encryption strategies, and shorter-term preservation requirements as well as permanent retention or destruction strategies must also be considered. Particular reference to data protection, privacy legislation, freedom of information, and environmental regulations requires organizations to know where their information is stored (in what jurisdictions) and how it can be accessed within given time frames. Will the move to the cloud restrict the organization's ability to comply?

Litigation also requires consideration: being able to identify relevant information, retrieve it,

Table 1. General pros and cons for moving to the cloud.

	Pro	Con
Reduced spending	Organizations purchase only the computing resources that they need; services are metered and billed on actual usage; in-house IT staff can be reduced or reassigned to focus on more business-critical tasks	Costs still involved in preparing for the cloud and implementing and configuring cloud services to integrate with existing business processes; ongoing management and monitoring of cloud services add to overall cost
Higher flexibility and scalability	Estimating and provisioning for peak computing resource demands eliminated; organizations can access virtually unlimited computing power and storage capacity; customers can scale up/down computing power depending on demand	Companies need to monitor usage to ensure that cloud service costs don't outweigh perceived benefits
Ease of use	Cloud services often require no more than a simple signature and can be accessed from anywhere via the Internet; no long-term commitment to the service required; standard interfaces are familiar to most users	Interoperability can become an issue when attempting to combine different cloud services, which might result in longer implementation time and higher cost
Improved reliability and security of scale	Server or virtualized instances' failures rarely affect provision; storage in multiple locations prevents loss of information; services offer greater resources for network and application security and greater expertise in security practice; cheaper and easier measures are possible on a larger scale; defensive measures are implemented quickly through virtualization and automation; early incident detection mechanisms reduce response times to breaches and incidents	Cloud providers do have outages, and resumption of services is out of customer's control; if cloud provider doesn't meet agreed availability service-level agreements, customers usually only receive free service time as compensation
Modernization of business processes	No proprietary licenses for business software; flexible mix of applications/services available to meet business needs on long- or short-term basis; customers can combine different cloud services; cloud facilitates collaborative work both internally and externally, plus the ability to collaboratively edit documents in real time	Innovative applications and services are built to suit a broad customer base and therefore lack the ability to customize to suit a specific organization's needs
Business continuity/ disaster recovery	Can facilitate business continuity and disaster recovery strategies; eradicates need for hardware for offsite replication and storage; improves the availability of information in the event of a disaster	Value-added services such as performance monitoring and the extra security that might be required to comply with legal and regulatory considerations add to overall cost

and supply it to courts in a timely manner can be difficult if the organization hasn't thought about how this would be achieved prior to an incident. Contracts need to be negotiated with these considerations in mind, with clauses built in about data destruction or how information can be returned to the organization, as well as how the provider manages it.

Operating in the Cloud

Use of information in the cloud typically precludes the use of encryption because it would adversely affect data processing, indexing, and searching. If the service uses encryption, the customer would need to know if this happens automatically and how the encryption keys are created, held, and used across single and multiple sites to be able to confirm that information is authentic. Business continuity can be affected by system failure, so information about continuity, monitoring, priority, and recovery procedures would give organizations a better picture of the risk of system failure to their activities.

Ultimately, making decisions about which cloud service/deployment model to select, and what sort of things to take into consideration when making that initial decision, requires the organization to consider whether loss of control will significantly affect the security of mission-critical information. In particular, identifying risk and assessing the organization's risk appetite is a critical factor in making decisions about moving to the cloud. The business must be clear about the type of information it's willing to store, how sensitive that information is, and whether its loss or compromise would affect the compliance environment in which the organization operates. □

Acknowledgments

More information about the research undertaken by Aberystwyth Univer-

Ten Questions to Ask When Outsourcing to the Cloud

Which processes, applications, or information can move to the cloud to improve efficiency and save money while still satisfying the organization's security and compliance requirements?

How can the organization be harmed if unauthorized people access the provider's systems, applications, services, or information and breached data is made available to the public?

How does the provider protect information and systems against unauthorized access (hacking, interception, user misuse)?

How can the organization ensure the integrity, authenticity, and reliability of information stored in the cloud?

What are the organization's responsibilities regarding the security of infrastructure and information in the cloud for the chosen cloud service and deployment models?

How can the organization apply its records and information management programs to the cloud environment?

What is the impact of outsourcing services and information to the cloud on the organization's legislative and regulatory requirements?

How should the organization audit and monitor cloud services and establish relevant service-level agreements?

Will the organization be able to negotiate contracts and agreements that fit its risk assessment and compliance environment?

What are the total costs of setting up and managing cloud services?

sity in conjunction with the Archives and Records Association of UK and Ireland, which underpins this article, can be found at www.archives.org.uk/ara-in-action/best-practice-guidelines.html.

Kirsten Ferguson-Boucher *lectures in records management; information governance; law, compliance, and ethics; and information assurance at Aberystwyth University, Wales. Her research interests include the convergence between related disciplines and how organizations in all sectors can reach acceptable levels of information governance and assurance across the spectrum of technologies. Contact her at knb@aber.ac.uk.*

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*